MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 3, 2022/2023

BCS2014 – CYBER SECURITY

(All sections/Groups)

6 OCTOBER 2023
9.00 a.m – 11.00 a.m
(2 Hours)

INSTRUCTIONS TO STUDENT

1. This question paper consists of 4 pages with 4 Questions only.
2. Attempt **ALL** questions. All questions carry equal marks and the distribution of the marks for each question is given.
3. Please write all your answers in the Answer Booklet provided.

SECTION A: Structured Questions (100 Marks)

QUESTION 1

Ransomware attacks: is there a case for paying up?

Victims choosing to pay out have incurred lower average breach costs than those who do not.

To pay or not to pay? For companies, which are unfortunate enough to be hit by a ransomware attack, that is the crucial question. Ransomware attacks in which cyber criminals lock up a victim's data or computer system and release it only if a ransom is paid exploded in 2020 and 2021, in part because a shift to remote working during the pandemic left organizations more vulnerable to hacking. But the tide appears to be turning. In its mid-year 2022 Cyber Threat Report, US security company Sonic-Wall identified a 23 per cent drop in the number of ransomware attempts. It attributed this to several factors including a "downward" trend in the number of organizations willing to pay cyber criminals.

That trend is borne out in the data gathered by those who help victims of ransomware handle the fallout. In 2019, 85 per cent of ransomware cases handled by cyber security group Coveware ended in a payment. But, in the first quarter of 2022, that proportion had fallen to 46 per cent. "The majority of the cases we handle do not end in a ransom," says Bill Siegel, Coveware's chief executive. He adds that many find ways to recover their data via backups or establish that certain data is not critical.

"It depends on whether you trust the criminals to delete stolen data. Which would be a big mistake" Brett Callow.

There are other factors at play in the slight decrease in ransomware attacks, too. For example, most hackers demand payouts in difficult-to-trace cryptocurrencies, but these have slumped in price this year, rendering the business of ransomware less lucrative.

Meanwhile, there has been increased government and law-enforcement focus on taking down ransomware criminals and the apparatus they use to support their business. This crackdown has come in the wake of several debilitating attacks on high-profile targets such as the Colonial Pipeline attack in 2021.Russia's invasion of Ukraine has also hit the sector, according to experts. Many Russian-based cyber hackers have turned their attention to attacks related to the conflict rather than ransomware or have had their operations disrupted by sanctions against Russia. Still, attacks continue to occur and the question of whether to pay ransomware hackers or not remains hotly debated.

Both the US and UK governments publicly recommend against it. They argue that it does not necessarily guarantee that victims will get their data or systems back, and also emboldens attackers by rewarding them, creating a vicious circle. Some authorities are becoming more vehement about outlawing the practice. The US states of North Carolina and Florida have now explicitly banned state and local government agencies from paying hackers. Pennsylvania, Texas, Arizona and New Jersey are exploring similar policies. New York is proposing banning businesses, as well as government agencies, from paying ransoms.

Continued...

Oren Wortman, vice-president of cyber security services for North America at cyber company Sygnia, recommends that business leaders conduct an "extensive risk assessment of cost benefit analysis of whether to pay or not". Decisions tend to be made on a case-by-case basis, he says, weighing up the price tag of the ransom demand against the potential cost of not paying, which could include loss of data, business disruption, or legal risk if customers decide to sue if their data gets leaked by the hackers. For example, he says "clients in the legal sector with confidential client data" often opt to pay to avoid the potential reputational hit to their firm. And in some cases, it may be cheaper to pay the ransom than to recover the data or systems from backups.

IBM Security's 2022 Cost of a Data Breach Report showed that the average breach costs for victims who opted to pay ransom demands were $630,000 lower than for those who chose not to pay. According to SonicWall, some victims have become more reluctant to pay due to growing awareness that many ransomware criminals are linked to Russia. Targets could therefore risk violating sanctions — and incurring civil penalties — if they sent them money. "Some [victims] may be worried that the money could fund the Russian government's actions, and object to paying a ransom on ethical grounds," SonicWall adds.

Others are skeptical of the hackers themselves. On average, in 2021, organizations that paid the ransom got back only 61 per cent of their data, with only 4 per cent able to retrieve all their data, according to a report by Sophos. Hackers could also sell or leak stolen data at a later point; there are no guarantees.

"The question of whether or not to pay depends on whether you trust the criminals to delete the stolen data, which would be a big mistake," says Brett Callow, threat analyst at the cyber security group Emsisoft.

Callow's company tries to help victims find ways to re-access their data without having to pay a ransom fee a tricky task, but one that can be possible if hackers have errors or weaknesses in their code. "It generally can't be made public knowledge because, if it did, the ransomware gang would realise it has a technical problem, so the word is spread quietly. This is why companies should go to law enforcement because they may be aware of a technical solution to the problem," he explains. Still, many experts warn that the total ransoms paid may be far higher than is currently known as there are no rules around disclosing payments.

Steve Tcherchian, chief information security officer at XYPRO, a cyber security solutions company, says that, in many cases, companies "don't have a choice but to pay a ransom". But he adds that "a lot of that is their own doing" due to lax cyber security practices. Having a clear incident response plan, and multiple backups of data is vital to guarding against having to pay out in the future, he says.

(*Source*: (2023). *Ransomware attacks: is there a case for paying up?*. Retrieved from https://www.ft.com/content/14de7a07-cc4f-483c-915f-d0b5cfc00a32)

Continued...

a. To pay or not to pay? This question of whether to pay ransomware hackers or not remains hotly debated in the article above.

(i) Which is your choice if you are one of the ransomware victims? Support your answer with the points from the article above.

(8 marks)

(ii) How can you negotiate your way out of a ransomware attack?

(6 marks)

b. Based on the article, in its mid-year 2022 Cyber Threat Report, US security company Sonic-Wall identified a 23 percent drop in ransomware attempts. Explain why?

(5 marks)

c. According to Steve Tcherchian, the chief information security officer at XYPRO, a cyber security solutions company, says that, in many cases, companies "don't have a choice but to pay a ransom." However, he adds that "a lot of that is their own doing" due to lax cyber security practices. Discuss how their cyber security team can improve cyber security education and awareness about ransomware attacks.

(6 marks)

(Total: 25 marks)

QUESTION 2

a. Define **THREE (3)** key concepts that form the CIA triad.

(9 marks)

b. A breach of data integrity in ACE Company can prevent them from conducting their business well. Identify **FOUR (4)** threats to the data integrity and **FOUR (4)** ways how to preserve their data integrity.

(16 marks)

(Total: 25 marks)

Continued...

QUESTION 3

a. Discuss **FIVE (5)** desired outcomes of information security governance and how such a program would benefit the organization.

(13 marks)

b. You are working at the Cyber Space Security Unit as a Chief Information Security Officer (CISO). Your responsibility is to develop a cyber security policy for your company.

(i) What is a cyber security policy? (2 marks)

(ii) Explain **THREE (3)** basic rules that you must follow when developing a cyber security policy.

(6 marks)

(iii) Why a clear cyber security policy is critical for companies? (4 marks)

(Total: 25 marks)

QUESTION 4

a. In security employment practices, how do the security considerations for temporary workers differ from those for regular employees?

(10 marks)

b. When an employee leaves an organization, what should the former employee do to reduce the risk of exposure to organizational information?

(15 marks)

(Total: 25 marks)

End of Paper